In the Claims:

Please amend claims 1, 5, 7, 9, 12-16 and 20, and add new claims 21-40 as follows:

1. (Currently Amended) A computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, causes a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; ~~and~~

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment ~~criteria.~~criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

2. (Currently Amended) The computer program according to claim 1, causes the computer to further perform changing the setting information upon it ~~is~~ being judged at the judging that the communication is executed by the worm, wherein

the acquiring includes acquiring the information based on the setting information after a change.

3. (Currently Amended) The computer program according to claim 1, causes the computer to further perform changing the judgment criteria upon it ~~is~~ being judged at the judging that the communication is executed by the worm, wherein

the judging includes judging whether the communication is executed by the worm based on the information acquired and the setting information after a change.

4. (Original) The computer program according to claim 1, wherein the judging includes judging that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

5. (Currently Amended) The computer program according to claim 4, wherein the judging includes judging that a communication from a plurality of computers in the predetermined segment is executed by the worm when

a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, and

the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside.

6. (Original) The computer program according claim 1, wherein the judging includes judging that a communication from a computer that is outside the predetermined network segment is executed by the worm when

there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and

there is an increase in number of sender addresses of the communication packets.

7. (Currently Amended) The computer program according to claim 1, wherein the judging includes outputting any one of information about a computer that performed the communication and a communication status upon it ~~is~~ being judged that the communication is executed by the worm.

8. (Original) The computer program according to claim 1, wherein the judging includes predicting a type of the worm by comparing features of a communication judged to be executed by a worm with features of a communication executed by a worm that is recorded in advance.

9. (Currently Amended) The computer program according to claim 1, causes the computer to perform cutting off the communication executed by the worm upon it ~~is~~ being judged that the communication is executed by the worm.

10. (Original) The computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by stopping a process that is started by the worm.

11. (Original) The computer program according to claim 9, wherein the cutting off includes cutting off the communication executed by the worm by making a fire wall function effective in a computer that is judged to have a worm.

12. (Currently Amended) A computer-readable recording medium for storing a computer program for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, the computer program causing a computer to perform:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; ~~and~~

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment ~~criteria.~~criteria;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

13. (Currently Amended) A method for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

acquiring information related to a traffic and a communication address of a communication packet based on setting information; ~~and~~

judging whether the communication is executed by the worm based on the information acquired and a predetermined judgment ~~criteria.~~criteria; and

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

14. (Currently Amended) A device for detecting a worm by monitoring a communication of a predetermined network segment that is connected to a network and judging whether the communication is executed by a worm, comprising:

an acquiring unit that acquires information related to a traffic and a communication address of a communication packet based on setting information; ~~and~~

a judging unit that judges whether the communication is executed by the worm based on the information acquired and a predetermined judgment ~~criteria.~~criteria;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged by the judging unit that the communication is executed by the worm; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted by the reference information extracting unit.

15. (Currently Amended) The device according to claim 14, further comprising a setting changing unit that changes the setting information upon it ~~is~~ being judged by the judging unit that the communication is executed by the worm, wherein

the acquiring unit acquires the information based on the setting information after a change.

16. (Currently Amended) The device according to claim 14, further comprising a setting changing unit that changes the judgment criteria upon it is judged by the judging unit that the communication is executed by the worm, wherein

the judging unit judges whether the communication is executed by the worm based on the information acquired by the acquiring unit and the setting information after a change.

17. (Original) The device according to claim 14, wherein the judging unit judges that a communication from a computer that is in the predetermined network segment is executed by the worm when

there is an increase in number of communication packets as well as number of destination addresses of communication packets that are transmitted from the predetermined network segment to the outside.

18. (Currently Amended) The device according to claim 17, wherein the judging unit judges that a communication from a plurality of computers in the predetermined segment is executed by the worm when

a communication from a computer in the predetermined network segment is judged previously to be executed by the worm, and

the number of destination addresses of the communication packet that is transmitted from the predetermined network segment to the outside becomes greater than a number of destination addresses of a communication packet acquired when the communication is judged to be executed by the worm, and is transmitted from the predetermined network segment to the outside.

19. (Original) The device according claim 14, wherein the judging unit judges that a communication from a computer that is outside the predetermined network segment is executed by the worm when

there is an increase in number of responding communication packets corresponding to communication packets that are transmitted from outside to the predetermined network segment, and

there is an increase in number of sender addresses of the communication packets.

20. (Currently Amended) The device according to claim 14, wherein the judging unit judges outputs any one of information about a computer that performed the communication and a communication status upon it ~~is~~ being judged that the communication is executed by the worm.

21. (New) The computer program according to claim 1, wherein the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

22. (New) The computer-readable medium according to claim 12, wherein the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

23. (New) The method of claim 13, wherein the extracting includes extracting as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging.

24. (New) The device according to claim 14, wherein the reference information extracting unit extracts, as a reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the judging unit.

25. (New) The computer program according to claim 1, wherein the extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value.

26. (New) The computer-readable medium according to claim 12, wherein the extracting further includes summing up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being

judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value.

27. (New) The method of claim 13, wherein the extracting further includes summing up, for each type of communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value.

28. (New) The device according to claim 14, wherein the reference information extracting unit further sums up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged that the communication is executed by the judging unit, and extracts, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value.

29. (New) The computer program according to claim 1, wherein the extracting further includes detecting address information of a worm-infected computer from a header of the communication packet transmitted in the communication

upon it being judged that the communication is executed by the worm at the judging, and extracting the address information as the reference information.

30. (New) The computer-readable medium according to claim 12, wherein the extracting further includes detecting address information of a worm-infected computer from a header of the communication packet transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting the address information as the reference information.

31. (New) The method of claim 13, wherein the extracting further includes detecting address information of a worm-infected computer from a header of the communication packet transmitted in the communication upon it being judged that the communication is executed by the worm at the judging, and extracting the address information as the reference information.

32. (New) The device according to claim 14, wherein the reference information extracting unit further detects address information of a worm-infected computer from a header of the communication packet transmitted in the communication upon it being judged that the communication is executed by the judging unit, and extracts the address information as the reference information.

33. (New) A device for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

a worm judging unit that judges whether a communication is executed by the worm;

a reference information extracting unit that extracts reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm; and

a blocking unit that blocks the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network segment based on the reference information extracted by the reference information extracting unit.

34. (New) The device according to claim 33, wherein the reference information extracting unit extracts, as the reference information, a most frequently appearing port number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm.

35. (New) The device according to claim 33, wherein the reference information extracting unit further sums up, for each type of the communication, a number of the communication packets transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts, as the reference information, a type of the communication wherein the number of the communication packets is over a threshold value.

36. (New) The device according to claim 33, wherein the reference information extracting unit further detects address information of a worm-infected computer from a header of the communication packet transmitted in the communication upon it being judged by the worm judging unit that the communication is executed by the worm, and extracts the address information as the reference information.

37. (New) The device according to claim 33, wherein the worm judging unit judges whether the communication is executed by the worm based on traffic of the communication packets transmitted in the communication.

38. (New) The device according to claim 33, wherein the worm judging unit judges whether the communication is executed by the worm based on the

information related to a communication address of a communication packet transmitted in the communication.

39. (New) A computer-readable recording medium for storing a computer program for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, the computer program causing a computer to perform:

judging whether a communication is executed by the worm;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.

40. (New) A method for cutting off a communication executed by a worm by monitoring the communication between a predetermined network segment and outside of the predetermined network segment, comprising:

judging whether a communication is executed by the worm;

extracting reference information for identifying a communication packet to be blocked from a plurality of communication packets transmitted in the communication upon it being judged at the judging that the communication is executed by the worm; and

blocking the communication packet that is transmitted between the predetermined network segment and the outside of the predetermined network based on the reference information extracted at the extracting.